新軟週報
HTTP WWW.NUSOFT.COM.TW
Internet Security Fighter
2009/8/10-2009/8/23 第98期

多功能 UTM / MS 系列報導

技術淺談與應用 - 認證上網所需注意的事項

公司內部的網路資源，若被員工拿來做為私人用途，不但會佔用到網路的頻寬進而也會影響到公司的產能，因此有規畫的網路運用對公司而言絕對是有必要的。

而新軟系統所推出的『多功能 UTM-MS』系列產品，內建了“認證上網”之功能，讓所有需使用網路資源的使用者都必須先通過認證才可使用，如此一來即可對公司內做初步的網路管理，同時也讓不必使用網路資源之相關部門能有進一步的管制。但身為網路管理人員，在做該項認證的設定時，又該留意到哪些問題呢？

首先管理人員所需先瞭解到的是使用者電腦 DNS 設定情況為何？而 DNS 設定情況又可分為下列兩種：

1.使用者電腦中的 DNS Server 指向 MS，由 MS 代為使用者 PC 去向外部的 DNS Server 做解析網域名稱的動作。

2.使用者電腦中的 DNS Server 指向外部，例如 HINET 的 DNS Server (168.95.1.1)。當使用此種設定時，則網路管理人員就必須要注意到 MS 中的管制條例設置。

因為 MS 上網的認證機制是利用 http 的 80 port 來做認證，但由於一般的使用者在上網時會習慣直接於網址列上輸入 Domain Name(例如 tw. yahoo. com)而非輸入 IP 位址(例如：119.160.246.241)，因此，在輸入 Domain Name 後還需要先藉由 DNS 的服務(53 port)來解析網域名稱，才能夠正常的經由 80 port(也就是 Http)來上網。因此當使用者為上述情況 1 時，則不必額外的考慮到上網做 DNS 解析時，是否會因為認證的限制，而無法正常的向外做解析的動作。但若為上述情況 2 時，則網路管理人員就得先確定管制條例中，是否有可供使用者能正確的連上 DNS 伺服器做解析的條例存在。若是沒有該項通過條例，就必須開一條讓 DNS 通過的管制條例。

MS 的管制條例特性為「由上而下」、「逐條比對」，當比對到有符合的管制條例時，系統便會套用該條管制條例。而當比對到有需要認證的管制條例時，系統會先向下比對看是否有可以允許放行的條例，若有，則會走下方條例出去。因此，在其認證的管制條例下方，需再設定一條阻擋的條例，用意為讓比對的動作到此為止，不再繼續向下做比對。

舉例來說，如有一位使用者 Andrew 必須要經過認證才能上網，而其他人則不需認證的情況。那麼於 MS 中 Policy 的設定如下：

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	DNS	✓		Modify Remove Pause	To 1
Andrew	Outside_Any	ANY	✓		Modify Remove Pause	To 2
Andrew	Outside_Any	ANY	✗		Modify Remove Pause	To 3
Inside_Any	Outside_Any	ANY	✓		Modify Remove Pause	To 4

認證上網 Policy 設定範例圖

管制條例順序	來源	目的	服務	管制動作	用意
1	inside any	outside any	DNS	允許	置頂的用意為，先讓欲作 DNS 解析之封包能通過。
2	andrew	outside any	ANY	認證	來源為 Andrew 這位使用者，必須要通過認證才可使用網路服務。
3	andrew	outside any	ANY	阻擋	因為使用認證的條例較特殊，故須在此多加一條條例做阻擋，讓來源為 Andrew 之使用者的封包不再繼續向下方其他管制條例做比對。
4	inside any	outside any	ANY	允許	讓其他非 Andrew 的使用者可以正常上網，同時不需經過認證。

Policy 設定說明表

另外還需要注意的是，當有使用外部 Proxy Server(代理伺服器)的時候，其 Proxy Server 上網所用到的 port 號不一定會是 80 port，因此需通過認證才能上網的使用者，則須手動輸入IP 位址(82 port)來認證上網，使用者可在瀏覽器上輸入「http://(MS 的 LAN Port IP) : 82/」進行認證。但 IE 在使用 Proxy Server 上網時，即使勾選了「近端網址不使用 Proxy」，IE 仍會無法正確分辨遠端和近端，所以當打上「http://(MS 的 LAN Port IP) : 82/」時 IE 會讓 Proxy Server 向外部 Internet 查詢該項 IP 位址，導致查無 IP 位址而無法認證。因此，解決方法，可使用 Firefox 瀏覽器，將「內部網段不使用代理伺服器」的功能開啟，便可順利的經由認證來上網。

文 陳殿鴻 kim@nusoft.com.tw

市場行銷報導 - 新軟多功能 UTM 有效管制員工上網聊天

拜網路科技發達所賜，從早期 ICQ 乃至近幾年的 Yahoo 即時通、MSN、Skype…等等，讓人人於現今這個“全民 e 化”的時代裡，至少有一個即時通帳號，可用於朋友間交換訊息、工作時方便業務上之聯繫與傳檔交換等等…，不僅可建立快速便利的溝通橋樑，而且也比講電話更能省下一筆費用開銷。不過有些公司漸漸地發現員工經常利用上班時間使用 IM 從事私人行為，所以便開始加以管制，甚至直接禁止此類軟體安裝。但是道高一尺、魔高一丈，因此有些人動腦筋設計出「Web IM」這種不需要安裝軟體只要靠網頁就能使用的即時通訊程式。

「提高員工產能、增益公司獲利」為現代企業營運法則之一，因此企業為了使員工專心於自己的工作崗位上，無不積極採用相關管理設備。而目前市場上相關上網管制設備對於 IM 的管制方法大多採“防堵 Port 號”之簡易方式來阻擋，可是如此之方式，僅能對不常易動 Port 號的 IM 或 Web IM 產生阻擋效果，倘若該程式後續所推出的新版本採用目前主流之“變動式 Port 號”機制的話，長時間下來自然是難以招架進而土崩瓦解，更別說管制變化性更大的「Web IM」。

擁有自家研發團隊的新軟系統，面對目前市場上不斷推出新版本之 IM 或 Web IM 的挑戰，皆以最嚴謹的態度、最縝密的心思來嚴陣以待。追求高效率的新軟多功能 UTM 產品大大有別於一般市售設備僅以“防堵 Port 號”簡易阻擋機制的方式，進而設計以新軟獨家阻擋機制將其阻擋：

＊關鍵字串特徵比對

此機制為新軟系統所獨家研發，針對目前一些主流的 IM 或 Web IM 所特別設計。而且完全不受制於該程式所使用哪個特定的 Port 號，即使該 Port 號會不斷地更換，新軟多功能 UTM 的管制效果依然不減，只因為新軟所採用的技術為在當傳送的封包送至設備端時，會將封包比對新軟獨家建立的“關鍵字串特徵資料庫”，若有符合 IM 關鍵字串特徵的封包，一律皆阻擋下來，其餘的正常的封包將予以放行。如此一來，在新軟多功能 UTM 網路架構底下，一般無予以授權使用 IM 即時通訊的員工，因為受到新軟多功能 UTM 的管制便無法使用 IM 即時通訊軟體，將能做到滴水不漏的管制機制。

有鑒於目前 Web IM 漸漸於網路上嶄露頭角，新軟系統早在此之前便以獨到的眼光發現問題之存在，並立即著力於開發此問題之解決方案。目前針對阻擋 Web IM 部分，新軟系統所推出的多功能 UTM 採用上述新軟獨家技術已能成功管制大多數 Web IM 的使用。目前新軟多功能 UTM 所能完整管制 Web IM 的網站如下：

MSN	people.live.com（官方網站）
	www.msn2go.com
	www6.messengerfx.com
Yahoo 即時通	webmessenger.yahoo.com (官方網站)
ICQ	icq2go (官方網站)
AIM	AIM Express (官方網站)
QQ	web.qq.com (官方網站)
All in 1 Web IM	iloveim.com (MSN、Yahoo 即時通、AIM)
	imo.im（MSN、Yahoo 即時通、ICQ、AIM)
	www.koolim.com（MSN、Yahoo 即時通、ICQ、AIM)
	www.meebo.com（MSN、Yahoo 即時通、ICQ、AIM)
	wablet.com（MSN、Yahoo 即時通、ICQ、AIM)
	www.ebuddy.com（MSN、Yahoo 即時通、ICQ、AIM)
	webuzz.im（MSN、Yahoo 即時通、AIM)
	www.imunitive.com（MSN、Yahoo 即時通、AIM)

然而人是會隨著時間而變化的，網路科技更是如此，各家 IM 業者為了追求品質更好、更方便的聊天環境，勢必會不斷地推出新版本的 IM 即時通訊程式。而面對各 IM 業者不停地推出之新版本 IM 的挑戰，新軟系統不畏網路世界潮流之變化，秉持著「兵來將擋、水來土淹」產品設研發理念，以堅強的技術研發團隊為後盾，推出一系列相關對應程式供用戶下載更新使用。

文 黃政銘 ming@nusoft.com.tw